Instructor
Liljana Babinkostova
liljanababinkostova@boisestate.edu
Office Location: MB 240B
Office Hours: Th 10:30 AM – 11:30 AM or by appointment
(208)426 – 2896

Course Description. Introduction to groups, fields and polynomial rings. The study of enciphering/deciphering and cryptanalysis of the Elliptic Curve, LUC, and NTRU public key cryptosystems. Group based authentication and digital signature schemes and anonymity protocols.

Prerequisite(s): MATH 187 or MATH 189.

About the Course. Cryptology is the science of writing and breaking codes. The science of writing secret codes is called cryptography and the science of breaking codes is called cryptanalysis. It is essentially impossible to do either cryptography or cryptanalysis well without having a good understanding of the methods of both areas. Historically, cryptography was used to ensure secret communication between two parties. Its scope has expanded nowadays and includes secure internet-wide communication, secure distributed computations, authentication, and more.

Every time you make a phone call, purchase with a credit card in a shop or on the web, get cash from an ATM, you use cryptography. Cryptography has specific security requirements, such as confidentiality, authentication, integrity and non-repudiation. To meet these security requirements, we employ private-key cryptography, public-key cryptography and hash functions.

This course will introduce you to group based public-key cryptography with the focus on elliptic curve cryptography. Since its introduction to cryptography more than 30 years ago, the elliptic curve cryptography (ECC) is increasingly gaining ground in the public-key cryptography protocol instantiation. Today it is most notably used in the implementation of Bitcoin crypto-currency. Transport layer security (TLS) protocol, secure shell (SSH) protocol and others include elliptic curves as viable options. The course will also introduce to lucas group cryptography and the NTRU encryption. We will learn about protocols that make data transmission secure, the importance of carefully designing cryptographic primitives, and techniques of breaking cryptographic schemas. We will not only cover these ideas in theory, but also give you a realistic exposure to the mathematics behind elliptic curve cryptology and the actual computational issues.

Along the way we’ll survey some mathematical topics as needed, including group theory, linear algebra, and the theory of cryptographic security.
Course Description

1. Introduction
   - Overview of Cryptology
   - Group Theory and Mathematical Background
   - Perfect Secrecy

2. Elliptic Curves
   - Elliptic curves as elementary equations
   - The algebraic structure of elliptic curves
   - Points on elliptic curves

3. Elliptic Curve Cryptography
   - Diffie-Hellman Key Exchange
   - Shamir-Massey-Omura encryption
   - Digital Signatures

4. Lucas Group Cryptography
   - Lucas sequences and functions
   - The algebraic structure of lucas sequences
   - Points on lucas curves
   - RSA Encryption using lucas groups

5. NTRU Cryptosystem
   - Polynomials and vector spaces
   - NTRU Public Key Encryption

Textbook. There is no textbook for the class. The lectures posted on the course web and the class notes are the main resources for studying the course. Any additional reading can be useful.

Recommended Textbooks


Web-Based Resources

- Cryptography I: Dan Boneh, Stanford University
  https://www.coursera.org/course/crypto

- Cryptography II: Dan Boneh, Stanford University
  https://www.coursera.org/course/crypto2
Elliptic Curves: Andrew Sutherland, MIT

Applied Cryptography: David Evans, University of Virginia
https://www.class-central.com/mooc/326/udacity-applied-cryptography

Grade Distribution

Assignments 50%
Quizzes 20%
Final Exam 30%

Letter Grade Distribution

$\geq 93.00$  A  $73.00 - 76.99$  C
$90.00 - 92.99$  A-  $70.00 - 72.99$  C-
$87.00 - 89.99$  B+  $67.00 - 69.99$  D+
$83.00 - 86.99$  B  $63.00 - 66.99$  D
$80.00 - 82.99$  B-  $60.00 - 62.99$  D-
$77.00 - 79.99$  C+  $\leq 59.99$  F

Course Policies

- **Final Exam**
  - The final exam will be an individualized take home exam. It will be posted at this website, and will be due within one week from the date of posting. Access to your exam will be restricted by a cryptographic key designed by you - according to specifications to be posted. The final exam will have points reserved for key-security (10% of the total points) and the remaining points will be for actual work handed in. All exams will be open to attack by the students enrolled in the class. A successful attack will result in the attacked not getting the key security points. The first two substantiated successful attackers per test will get bonus points.
  - For successfully attacking an exam the first attacker receives 5% of the total points extra credit and the second attacker receives 2.5% of the total points extra credit.
  - Any student may attack any number of tests. More details and restrictions will be posted in due time on the examination page.
  - **No makeup final exams will be given.**

- **Quizzes**
  - Three in class quizzes will be given throughout the semester. They will be team-based and consist of one problem and several multiple choice questions. Each quiz will be 30-40 minutes long. The goal of this component of the course is to simulate the real world practice of cybersecurity, where teams of people with different backgrounds contribute to the common objective of analyzing and solving a cryptology related cybersecurity problem.
  - **No makeup quizzes will be given.**

- **Assignments**
Assignments are due by the posted due date at the beginning of class.

Although the course website provides computer implementations for topics covered in class, some assignments may require additional programming and/or use of resources available on the Internet. Each assignment must have two parts: Part 1 should be a summary of results and description of the strategy for solving the assigned problems. Referenced work must be clearly documented, cited, and attributed. Part 2 should contain only the computation work (Sage, Python, Matlab, Java, C or other programming language), annotated with appropriate commentary which describes the parts of the computation to the reader. Where appropriate, the student should also include any relevant web resources that are referenced in Part 1.

If the assignment involves programming, having only one of the two parts of the assignment will result in losing 20% of the total points available for the assignment.

Each student has an allowance of 4 late homeworks throughout the semester provided these are handed in within 24 hours of the due time.

No additional late assignments will be accepted.

• Grades

Grades in the C range represent performance that meets expectations; Grades in the B range represent performance that is substantially better than the expectations; Grades in the A range represent work that is excellent.

• Attendance and Absences

Attendance is expected and will be taken each class.

Students are responsible for all missed work, regardless of the reason for absence. It is also the absentee’s responsibility to get all missing notes or materials.

Academic Honesty Policy

• Students are expected to work independently. Offering and accepting solutions from others is an act of plagiarism, which is a serious offense and all involved parties will be penalized according to the BSU Academic Honesty Policy. Discussion amongst students is encouraged, but when in doubt, direct your questions to me.

• Referenced work must be clearly documented, cited, and attributed. Even in the case of work licensed as public domain or Copyleft, (see http://creativecommons.org/) the student must provide attribution of that work in order to uphold the standards of intent and authorship.